

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION**

IN RE: CAPITAL ONE CONSUMER)
DATA SECURITY BREACH LITIGATION) MDL No. 1:19md2915 (AJT/JFA)

**AMAZON’S RESPONSE IN SUPPORT OF
MOTION TO FILE UNDER SEAL**

Defendants, Amazon.com, Inc., and Amazon Web Services, Inc. (together, “Amazon”), by counsel and pursuant to Local Civil Rule 5 of Local Rules for the United States District Court for the Eastern District of Virginia, file this response in support of Plaintiffs’ Motion to File Under Seal. Dkt. 2099.

On November 5, 2021, Plaintiffs filed a redacted Memorandum in Support of Plaintiffs’ Motion to Compel Response to Plaintiffs’ Interrogatory No. 22 to AWS (“Memorandum”) and Exhibits D–K, O, Q, and T thereto under seal. Dkt. 2097. Plaintiffs lodged the unredacted copies of these documents with the Court as sealed filings. Dkt. 2103. Plaintiffs filed a Motion to file under seal portions of the Memorandum and Exhibits D–K, O, Q, and T and a notice of filing under seal as required by Local Civil Rule 5. *See* Dkt. Nos. 2099 & 2102.

The Memorandum and exhibits that are the subject of Plaintiffs’ Motion to File Under Seal include documents or references to documents designated as “Confidential,” “Confidential – Outside Counsel Only,” or “Confidential – Outside Counsel Only – Security Sensitive” pursuant to the Amended Stipulated Protective Order (Dkt. 368), and pertain to Amazon and Capital One’s sensitive security information, the public disclosure of which would be harmful to their interests.

Amazon respectfully submits that Exhibits D–K, O, Q, and T and designated excerpts of the Memorandum and should remain sealed because unsealing would disclose Amazon’s and Capital One’s confidential information related to security, which would cause competitive injury to both parties.

I. THE PROCEDURAL REQUIREMENTS FOR SEALING HAVE BEEN MET.

Under the local rules of this Court, a party may file a motion to seal together with the proposed sealed filings. Local Civ. R. 5(C). The Court will subsequently determine whether the sealing or redactions are proper.

A “trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests.” *In re Knight Publ’g Co.*, 743 F.2d 231, 235 (4th Cir. 1984). Before documents within a case may be filed under seal in the Fourth Circuit, the parties must: (1) provide notice to the public and give the public an opportunity to object to the sealing; (2) consider less drastic alternatives; and (3) provide specific findings in support of the decision to seal and the rejection of alternatives. *Ashcraft v. Conoco, Inc.*, 218 F.3d 282, 288 (4th Cir. 2000). All of these prerequisites are satisfied here.

First, the Court must provide notice of a request for sealing in the court record and provide interested persons with “an opportunity to object.” *In re Knight*, 743 F.2d at 235. The Court does not need to provide notice to the public of each document to be sealed where such individual notice would be “impractical” and “unwarranted,” as is the case here. *Id.* It is sufficient to docket the notice “reasonably in advance of deciding the issue.” *Id.* In accordance with Local Civil Rule 5, Plaintiffs’ sealing motion was publicly docketed, with a notice filed stating that any party or nonparty could object (Dkt. No. 2102).

Second, the Court must consider less drastic alternatives such as redactions or limited sealing. Here, less drastic alternatives to filing under seal are inappropriate. Although Plaintiffs took care to only redact their Memorandum as necessary to protect information that was properly designated Confidential, no other procedure other than filing under seal will be sufficient to preserve the confidentiality of the exhibits and the sensitive information discussed in the Memorandum. Sealing the exhibits noted below is necessary to avoid the public disclosure of confidential information including documents and deposition testimony related to AWS threat detection, a white paper that describes security configurations of AWS services used by Capital One, and other security information. *See, e.g., Walker Sys., Inc. v. Hubbell, Inc.*, 188 F.R.D. 428, 429 (S.D. W. Va. 1999) (stating “[w]here . . . the information sought to be protected concerns documents that the parties in good faith believe contain trade secrets or other confidential information, and the orders are routinely agreed upon by the parties, such orders should be granted”) (citing *Bayer AG & Miles, Inc. v. Barr Labs, Inc.*, 162 F.R.D. 456, 465 (S.D.N.Y. 1995); Fed. R. Civ. P. 26(c)).

Third, the Court must make specific findings, supported by the record, that justify sealing based on either the First Amendment or common law. It is well-settled that there is a public right of access to “judicial records.” *See Nixon v. Warner Commc’ns, Inc.*, 435 U.S. 589, 597 (1978). The public right of access may be based on the common law or the First Amendment. The common law right of access applies to “all judicial records and documents,” while the First Amendment right of access applies “only to particular judicial records and documents” – such as exhibits filed in connection with plea hearings and sentencing hearings in criminal cases, and trial proceedings and dispositive motions in civil cases. *Stone v. Univ. of Maryland Med. Sys. Corp.*, 855 F.2d 178, 180–81 (4th Cir. 1988). When, as here, confidential

materials are filed with the court to permit determination of a non-dispositive discovery motion, a common law right of access attaches to those filings. *See Anderson v. Cryovac, Inc.*, 805 F.2d 1, 10–13 (1st Cir. 1986). When the common law attaches, Courts routinely seal documents containing confidential business information and proprietary knowledge. *See, e.g., In re Knight*, 743 F.2d at 235 (discussing *Nixon*, 435 U.S. at 598 and how sealing is appropriate to avoid “unfairly gaining a business advantage”); *Padco Advisors, Inc. v. Omdahl*, 179 F. Supp. 2d 600, 614 (D. Md. 2002) (sealing documents that contain “valuable trade secrets”); *Walker Sys., Inc. v. Hubbell, Inc.*, 188 F.R.D. at 429–30 (granting motion to seal documents containing trade secrets and other confidential information).

The Memorandum and exhibits contain technical security information, which constitutes highly confidential and proprietary business information. These exhibits contain highly sensitive information that implicates Amazon’s and Capital One’s confidential and proprietary information, including non-public security practices. The Memorandum references, quotes from, or discusses information from these exhibits.

This information has not been made public. And the general public would have little interest in the information because it was generated by, and relates to, the internal activities of private entities and individuals. *See, e.g., Crum & Crum Enters. v. NDC of Cal.*, No. 09-145 (RBK), 2011 U.S. Dist. LEXIS 24690, at *12 (D. Del. Mar. 11, 2011). Accordingly, under the common law standard, Amazon’s strong interest in preserving the confidentiality of its proprietary business information justifies the sealing of portions of the Memorandum and Exhibits D–K, O, Q, and T. Sealing judicial records to protect sensitive business information is appropriate to prevent court files from becoming “sources of business information that might harm a litigant’s competitive standing.” *See Nixon*, 435 U.S. at 598.

II. AMAZON’S CONFIDENTIAL BUSINESS INFORMATION SHOULD BE SHIELDED FROM PUBLIC ACCESS.

A district court may order a filing to be sealed where it contains confidential business information. In fact, a corporation’s confidential information is considered a type of property to which the corporation has an exclusive right and benefit. *See e.g. Carpenter v. United States*, 484 U.S. 19, 26 (1987). The public right of access must give way to protect the confidential business information of parties in judicial filings. *See, e.g., Nixon*, 435 U.S. at 598; *In re Knight*, 743 F.2d at 235 (sealing court records is permissible to prevent others from “gaining a business advantage” from materials filed with court). As detailed below, the redacted portions of the Memorandum and Exhibits D–K, O, Q, and T contain confidential security information that could harm Amazon and Capital One if filed publicly. Accordingly, the Court should seal the exhibits and the unredacted version of the Memorandum, as they contain confidential business information that should be shielded from public access.

A. APPLICATION OF LAW TO THE SEALED EXHIBITS D–K, O, Q, T, AND REDACTED MEMORANDUM.

Exhibit D: This sealed exhibit is a letter from John Yanchunis to Tyler Newby, dated December 15, 2020. The information contained in this exhibit is confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-public details regarding Amazon’s cybersecurity practices. This exhibit contains references to and quotes from deposition testimony and documents that Amazon designated as “Confidential” pursuant to the Amended Stipulated Protective Order and that discuss non-public details about the technical investigation into the cyber incident, possible exfiltration paths used by the hacker, and Amazon’s confidential threat intelligence gathering practices.

As Steve Schuster, Director of Security Engineering and Response with Amazon Web Services, Inc., explains in his Declaration in support of Amazon's Confidential Memorandum in Support of Motion to Seal (Dkt. 1992), the information contained in this exhibit regarding Amazon's security threat intelligence practices is confidential and competitively sensitive. *See* Dkt. 1992 ("Schuster Decl.") ¶ 2. Threat intelligence methods and strategies, even at a high level, are not disclosed to the public because they could provide adversaries with a roadmap to evading Amazon's defenses. *Id.* Disclosure of this information will make these practices less effective for threat intelligence, compromising Amazon's security. *Id.*

The public disclosure of this exhibit could compromise Amazon's overall security and cause it competitive injury. There is little or no reason this exhibit should be disclosed to the public.

Exhibit E: This sealed exhibit is a letter from John Yanchunis to Tyler Newby, dated January 11, 2021. The information contained in this exhibit is confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-public details regarding Amazon's cybersecurity practices. This exhibit contains references to and quotes from documents that Amazon designated as "Confidential" pursuant to the Amended Stipulated Protective Order and that discuss non-public details about the technical investigation into the cyber incident as well as confidential information about other non-party AWS customers. The public disclosure of this exhibit could compromise Amazon's and its customers' overall security and cause them competitive injury. Thus, there is no reason that this exhibit should be disclosed to the public.

Exhibit F: This sealed exhibit contains meet and confer emails between Plaintiffs and Amazon, dated January and February 2021. The information contained in this exhibit is

confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-public details regarding Amazon's cybersecurity practices. This exhibit contains references to and quotes from deposition testimony and documents that Amazon designated as "Confidential" pursuant to the Amended Stipulated Protective Order and that discuss non-public details about the technical investigation into the cyber incident as well as confidential information about other non-party AWS customers. The public disclosure of this exhibit could compromise Amazon's and its customers' overall security and cause them competitive injury. Thus, there is no reason that this exhibit should be disclosed to the public.

Exhibit G: This sealed exhibit is Plaintiffs' Fourth Notice of Videotaped Deposition of Amazon.com and Amazon Web Services, Inc., dated February 10, 2021. The information contained in this exhibit is confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-public details regarding Amazon's cybersecurity practices. This exhibit contains references to and quotes from documents that Amazon designated as "Confidential" pursuant to the Amended Stipulated Protective Order and that discuss non-public details about the technical investigation into the cyber incident, Amazon's cybersecurity tools, and Amazon's confidential threat intelligence gathering practices.

The information contained in this exhibit regarding Amazon's security threat intelligence practices is confidential and competitively sensitive. *See* Schuster Decl. ¶ 2. Threat intelligence methods and strategies, even at a high level, are not disclosed to the public because they could provide adversaries with a roadmap to evading Amazon's defenses. *Id.* Disclosure of this information will make these practices less effective for threat intelligence, compromising Amazon's security. *Id.*

The public disclosure of this exhibit could compromise Amazon's overall security and cause it competitive injury. There is little or no reason this exhibit should be disclosed to the public.

Exhibit H: This sealed exhibit contains instant messages between AWS employees; AWS_CAP00068679. This document was designated "Confidential" by Amazon pursuant to section VII. B. of the Amended Stipulated Protective Order.

The information contained in this exhibit is confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-public details regarding Amazon's cybersecurity practices. This specific exhibit discusses the technical investigation into the cyber incident and investigations of other non-party AWS customers' environments. The public disclosure of this exhibit could compromise Amazon's overall security and cause competitive injury to both Amazon and its customers. There is no reason this exhibit should be disclosed to the public.

Exhibit I: This sealed exhibit is an excerpt from the transcript of the deposition of Amazon Rule 30(b)(6) witness Justin Christian, taken on February 18, 2021. This excerpt was designated as "Confidential" pursuant to section VII. B. of the Amended Stipulated Protective Order.

This exhibit includes confidential and non-public testimony regarding Capital One's use of Amazon's services. The specific testimony that is cited by Plaintiffs discusses confidential and/or competitively sensitive information regarding data reviewed by Amazon during its investigation of the breach. The public disclosure of this exhibit could compromise Amazon's cause competitive injury to both Capital One and Amazon. There is little or no reason this exhibit should be disclosed to the public.

Exhibit J: This sealed exhibit is a letter from John Yanchunis to Tyler Newby, dated March 2, 2021. The information contained in this exhibit is confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-public details regarding Amazon's cybersecurity practices. This exhibit contains references to and quotes from deposition testimony and documents that Amazon designated as "Confidential" pursuant to the Amended Stipulated Protective Order and that discuss non-public data reviewed by Amazon during its investigation of the cyber incident as well as Amazon's cybersecurity tools as employed by its customers like Capital One. The public disclosure of this exhibit could compromise Amazon's overall security and cause competitive injury to both Amazon and Capital One. There is little or no reason this exhibit should be disclosed to the public.

Exhibit K: This sealed exhibit contains emails regarding discovery between Plaintiffs and Amazon from March 2021. The information contained in this exhibit is confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-public details regarding Amazon's cybersecurity practices. This exhibit contains references to and quotes from deposition testimony, documents, and discovery responses that Amazon designated as "Confidential" pursuant to the Amended Stipulated Protective Order and that discuss non-public details from Amazon's investigation of the cyber incident. The public disclosure of this exhibit could compromise Amazon's overall security and cause competitive injury to both Amazon and Capital One. There is little or no reason this exhibit should be disclosed to the public.

Exhibit O: This sealed exhibit is a letter from John Yanchunis to Tyler Newby, dated September 7, 2021. The information contained in this exhibit is confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-

public details regarding Amazon's cybersecurity practices. This exhibit contains references to and quotes from deposition testimony and discovery that Amazon designated as "Confidential" pursuant to the Amended Stipulated Protective Order and that discuss non-public details from Amazon's investigation of the cyber incident. The public disclosure of this exhibit could compromise Amazon's overall security and cause competitive injury to both Amazon and Capital One. There is little or no reason this exhibit should be disclosed to the public.

Exhibit Q: This sealed exhibit is a non-public, security sensitive whitepaper entitled "Mitigating S3 Data Exfiltration Risks." This exhibit includes confidential, proprietary information, including: (1) specific details regarding exfiltration controls; (2) descriptions of Amazon services and products utilized by Capital One; (3) highly sensitive information regarding AWS's cybersecurity infrastructure and cloud environment; and (4) references to other AWS customers and their cybersecurity configurations. This exhibit is a confidential internal document shared only with Capital One which discusses proposed security features that are under development and have not been launched.

The public disclosure of this exhibit could compromise Amazon's overall security and cause competitive injury to both Amazon and Capital One. There is little or no reason this exhibit should be disclosed to the public.

Exhibit T: This sealed exhibit contains email communications between AWS employees; AWS_CAP00030314. This document was designated "Confidential" by Amazon pursuant to section VII. B. of the Amended Stipulated Protective Order.

The information contained in this exhibit is confidential and/or competitively sensitive, and public disclosure of this exhibit could provide outsiders with non-public details regarding Amazon's cybersecurity practices. This specific exhibit discusses the technical investigation

into the cyber incident and confidential Amazon cybersecurity policies. Therefore, public disclosure of the exhibit could compromise Amazon's overall security and cause competitive injury to both Amazon and Capital One. There is little or no reason this exhibit should be disclosed to the public.

Redacted Memorandum: The redacted portions of Plaintiffs' Memorandum [Dkt. 2097] cite to and incorporate information from Exhibits D–K, O, Q, and T, including quotes and summaries of confidential and/or competitively-sensitive information. Filing an un-redacted version of the Memorandum would be as injurious to Amazon as would be unsealing the Exhibits. Amazon thus requests that the un-redacted Memorandum remain filed under seal.

CONCLUSION

Accordingly, protecting Amazon's confidential, proprietary, and sensitive business information justifies sealing these materials that were filed in connection with Plaintiffs' Motion to File Under Seal. Amazon respectfully requests that Plaintiffs' Motion to Seal be granted consistent with the proposed order attached hereto, and the identified excerpts be sealed.

November 12, 2021

Respectfully submitted,

/s/ Robert R. Vieth

Robert R. Vieth, Esq. (VSB No. 24304)

HIRSCHLER FLEISCHER, PC

8270 Greensboro Drive, Suite 700

Tysons Corner, VA 22102

T: (703) 584-8366

F: (703) 584-8901

Email: rvieth@hirschlerlaw.com

*Local counsel for Defendants Amazon.com, Inc. and
Amazon Web Services, Inc.*

Tyler G. Newby (admitted *pro hac vice*)

Brian Buckley (admitted *pro hac vice*)

Laurence F. Pulgram (admitted *pro hac vice*)

Jedediah Wakefield (admitted *pro hac vice*)

Vincent Barredo (admitted *pro hac vice*)

Andrew M. Lewis (admitted *pro hac vice*)

Janie Y. Miller (admitted *pro hac vice*)

Meghan E. Fenzel (admitted *pro hac vice*)

Sarah V. Lightstone (admitted *pro hac vice*)

Rina Plotkin (admitted *pro hac vice*)

FENWICK & WEST LLP

555 California Street, 12th Floor

San Francisco, CA 94104

Telephone: (415) 875-2300

Facsimile: (415) 281-1350

Email: tnewby@fenwick.com

bbuckley@fenwick.com

lpulgram@fenwick.com

jwakefield@fenwick.com

vbarredo@fenwick.com

alewis@fenwick.com

jmiller@fenwick.com

mfenzel@fenwick.com

slightstone@fenwick.com

rplotkin@fenwick.com

*Counsel for Defendants Amazon.com, Inc. and
Amazon Web Services, Inc.*

CERTIFICATE OF SERVICE

I hereby certify that on November 12, 2021, I electronically filed the foregoing document **Amazon's Memorandum in Support of Plaintiffs' Motion to File Under Seal** with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Robert R. Vieth

Robert R. Vieth, Esq. (VSB No. 24304)

HIRSCHLER FLEISCHER, PC

8270 Greensboro Drive, Suite 700

Tysons, Virginia 22102

T: (703) 584-8366

F: (703) 584-8901

Email: rvieth@hirschlerlaw.com

*Local Counsel for Defendants Amazon.com, Inc.
and Amazon Web Services, Inc.*